ISSN: 1697-4328

RECIBIDO: 30/10/07
REVISADO: 20/11/07
ACEPTADO: 03/07/08

LA CRIPTOGRAFÍA DIPLOMÁTICA MEXICANA EN LA PRIMERA MITAD DEL SIGLO XIX. TRES EJEMPLOS

MEXICAN DIPLOMATIC CRYPTOGRAPHY IN THE FIRST HALF OF THE 19th CENTURY. THREE EXAMPLES

ROBERTO NARVÁEZ
Universidad Nacional Autónoma de México

Resumen: Descripciones y análisis de tres ejemplos de la criptografía diplomática que se usó en México entre 1824 y 1830.
Palabras clave: Criptografía, diplomacia mexicana, siglo XIX.

Abstract: Descriptions and analyses of three kinds of cryptosystems that Mexican diplomats used between the years 1824 and 1830.
Keywords: Cryptography, Mexican diplomacy, 19th century.

INTRODUCCIÓN

Los historiadores de la criptología no suelen investigar las pruebas del recurso a las comunicaciones secretas en lo que actualmente constituye el territorio de la República Mexicana. Es lo justo recordar que más de uno contribuyó al estudio del *nomenclator* utilizado por Hernán Cortés en 1532 y 1533 para encubrir ciertas fracciones de dos cartas enviadas a Francisco Núñez, su abogado *ad litem* ante la corte española.[1] Sin embargo, tales contribuciones resultan pertinentes a la historiografía criptológica de la Nueva España (por extensión, de la América colonial), pero no a la del México independiente. Ahora, lo cierto es que desde 1821 muchos ciudadanos mexicanos, atendiendo a muy variadas razones (políticas,

[1] G. LOHMANN VILLENA, "Cifras y claves indianas. Capítulos provisionales de un estudio sobre criptografía indiana", *Anuario de Estudios Americanos*, XI (1954), p. 304, nota 41; "Documentos cifrados indianos", *Revista de Indias*, 15 (1955), pp. 255-282, pp. 260-268 (Apéndice I); J. C. GALENDE DÍAZ, "Sistemas criptográficos empleados en Hispanoamérica", *Revista complutense de historia de América*, 26 (2000), p. 62, nota 23; R. NARVÁEZ, "Historia y criptología: reflexiones a propósito de dos cartas cortesianas", *Estudios de historia novohispana*, 36 (2007), pp. 17-62.

militares, diplomáticas, comerciales, etcétera), han apelado a diversos métodos para volver inmediatamente ilegibles sus escritos salvo para quien esté autorizado a leerlos; así lo deja patente la identificación y lectura cuidadosa de numerosos registros en diferentes archivos de México y el extranjero. En semejantes condiciones, parece obvio que nada falta salvo imaginación, un sentido lógico-crítico de los métodos historiográficos y las técnicas criptoanalíticas, y, en general, una voluntad científica, para fundar e impulsar el análisis comprensivo de los códigos y los criptosistemas cuya utilización por los mexicanos fue constante hasta por lo menos la década de 1930, cuando la mayoría de los métodos criptográficos eran todavía manuales en gran medida. Por supuesto, fomentar este género de inquisición documental necesariamente habrá de repercutir en un enriquecimiento de las historias generales de la criptografía, supliéndoles uno de los capítulos que de ordinario faltan en las mismas.

En un intento de poner en marcha esta particular empresa intelectual, ofrezco enseguida una serie de breves análisis y comentarios históricos y técnicos a tres ejemplos de la criptografía diplomática mexicana que surgieron entre 1824 y 1831.

1. EL CASO DE JOSÉ MARIANO MICHELENA, AGENTE CONFIDENCIAL EN INGLATERRA (1824)

Cuando una colonia proclama su independencia política respecto de la nación bajo cuyo imperio ha vivido durante siglos, algunos países de la comunidad internacional reconocen de inmediato su derecho a existir como un estado nuevo, libre y soberano. Pero siempre hay otros miembros de dicha comunidad que por motivos geopolíticos, económicos o de otra índole tardan en decidir si deben o no reconocer como válida esa misma proclama independentista. Es lo que le sucedió a la Nueva España después de que su guerra emancipadora contra el imperio español culminó con éxito en 1821. Por supuesto, a la cabeza de las potencias que se negaron a felicitar al recién nacido gobierno de los Estados Unidos Mexicanos se colocó España; esta situación se invirtió hasta 1836, después de varios intentos fracasados de reconquista y mucha tirantez diplomática. Sin embargo, para los intereses más estrictamente vitales de México durante los años inmediatamente posteriores a 1821, lo urgente a conseguir era el reconocimiento de Estados Unidos de América y de Inglaterra.

Consideremos en exclusiva las acciones diplomáticas que se realizaron para alcanzar la meta deseada respecto a Inglaterra. Este país se había reservado su proceder acerca de la independencia mexicana, esperando a ver las ventajas que España pudiese obtener de sus negociaciones con los autoproclamados nuevos Estados americanos.[2] Pero ese tipo de paciencia no convenía al gobierno mexicano, y por ello decidió enviar un agente confidencial a Londres para negociar directamente a favor de la causa mexicana. El Congreso aprobó entonces el nombramiento de José Mariano Michelena como tal agente el 4 de marzo de 1824. El promotor principal de la misión fue el secretario del Despacho de Relaciones Interiores y Exteriores, Lucas Alamán y Escalada (1792-1853).[3] Los historiadores han estudiado mucho la obra historiográfica y el legado político de Alamán, sin embargo, nadie hasta hoy se ocupó en investigar su recurso a la criptografía mientras fungió como canciller. Atendió esa cartera en cinco términos distribuidos en nueve años. El segundo cubrió del 15 de mayo al 21 de septiembre de 1824, época en la que fue responsable de dirigir los pasos de Michelena por las altas esferas de la diplomacia inglesa.[4] Para ello convino con su subordinado en utilizar un criptosistema de cierta clase con el fin de robustecer lo más posible la seguridad de su mutua correspondencia oficial.

Michelena remitió un primer informe cifrado sobre sus avances el 3 de julio de 1824. Siguieron tres mensajes, igualmente velados, con las fechas respectivas 17, 27 y 31 del mismo mes.[5] Por su parte, Alamán le hizo llegar una minuta en cifra fechada el 12 de julio —cuyo texto plano ha sido impreso en diversas compilaciones de documentos, y bajo tal forma revisado extensamente por los historiadores de la diplomacia.[6] En la minuta referida el canciller Alamán expone las es-

[2] L. ALAMÁN, *Historia de Méjico*, México, 1985-1986, t. V, pp. 469-470.

[3] A. SÁNCHEZ ANDRÉS, "De la independencia al reconocimiento. Las relaciones hispanomexicanas entre 1820 y 1836", en *México y España en el siglo XIX. Diplomacia, relaciones triangulares e imaginarios nacionales*, México, 2003, pp. 23-51.

[4] O. GUERRERO, *Historia de la Secretaría de Relaciones Exteriores*, México, 1993, pp. 22-23.

[5] E. GÓMEZ de la PUENTE (editor), *La diplomacia mexicana*, México, 1913, vol. 3., pp. 26, 103-104.

[6] AA. VV., *México y Cuba. Dos pueblos unidos en la historia*, México, 1982, vol. I, pp. 26-27; E. GÓMEZ de la PUENTE (editor), *La diplomacia mexicana...*, vol. 3, pp. 40-41. En éste último volumen se sugiere que esta nota representa el pliego de las instrucciones oficiales respecto al Tratado y Reconocimiento de la Independencia, por ello la imprimen como anexo al decreto del congreso mexicano aprobando el nombramiento de Michelena (impreso, sin fecha, en las páginas 103-104). Comparte la idea A. de la PEÑA y REYES, *Lucas Alamán. El reconocimiento de nuestra independencia por España y la unión de los países hispanoamericanos*, México, 1924, p. XII. Por su parte, los editores del volumen *México y Cuba* (vol. I, p. 27) piensan que las mencionadas instrucciones fueron remitidas a Michelena hasta octubre de 1824. En mi opinión, para disipar esta

trategias a seguir —de preferencia en un frente común con los representantes diplomáticos de otros países americanos, especialmente Argentina, Colombia y Chile— a propósito de un proyecto inglés para signar un tratado sobre el reconocimiento de las independencias americanas.

Ahora, cuando Alamán dejó la Secretaria del Despacho de Relaciones Interiores y Exteriores por segunda ocasión, Michelena persistía en la estrategia ordenada. Lo notificó así en carta del 6 de noviembre de 1824,[7] la cual se recibió en México hasta principios de febrero de 1825, por tanto, casi un mes después de que Alamán hubiera regresado a la cancillería por tercera ocasión. Probablemente, pues, fue con el documento en cuestión que se reanudó la correspondencia oficial cifrada entre nuestros dos personajes. Transcribiré parcialmente la carta originalmente cifrada:

M m h x e h r h c f u g f s g f r q f u x s r t b i m t b o n m g q r
d l z u o d d i c d z d i g j u l d p x l m x t n z x l i m s h i m o
f g j q x s q l c e r o y i i u b x h x f q x s e r q f u x s e
x q g z x u b x p x l t e m f y j b f z d t d m l g e m
i m r o z q d t j b l l m q n s n o m m o l l e s c v h x f i i m i
i x l j v i h i y q p a l j a z m j e e y q y h i j v l h y q l g i l l a
i m v a y q e z m f q v m o y a a y u v d m i l g e
t j l l q r d r a v r p i g h s n x f u x l u y h v f

Al descifrar este fragmento[8] leemos la cadena sintagmática:

He comunicamo (*sic*) a los ministros de colombia
Y chile y al que dyrige los asuntos de buenos
Ayres mis pasos dados con este ministe
rio todos los han aprobado y estan
de acurdo (*sic*) Estamos igualmente conveni
dos en que si ynglaterra sigue en su sistema
De entretenernos urgire hasta

duda es necesario, antes que otra cosa, realizar una seria investigación criptológica de toda la documentación pertinente.

[7] Acervo Histórico Diplomático de la Secretaría de Relaciones Exteriores de México (en adelante AHDSREM), Folio 1-1-44, "1822-25. Reconocimiento de la Independencia de México por Inglaterra", ff. 81-82 (el principal de la nota).

[8] En este escrito siempre citaré como texto plano recuperado lo que el estricto proceso de desciframiento me devolvió, realizando cero modificaciones en todos los casos.

Obtener una decision positiva

Se trata de un ejemplar de cifra o criptosistema cuya transformación dependió de la sustitución polialfabética. El afán de incrementar la seguridad es el principal motivo de optar por un método semejante, pues al utilizar varios alfabetos en lugar de uno solo durante la sustitución —como se hace, por definición, en los criptosistemas monoalfabéticos—, las frecuencias relativas de los caracteres en el criptotexto y el texto plano exhiben distribuciones diferentes; en términos prácticos, esto significa que a todo eventual criptoanalista le resultará imposible detectar una correspondencia de uno a uno —en teoría, por lo menos— entre los respectivos caracteres del criptograma y del texto plano, viéndose obligado, entonces, a seleccionar un método de "ataque" (como se dice en el argot criptológico) diferente al análisis de frecuencias relativas[9] y, por implicación lógica, deberá ceñirse a uno o varios modos de razonamiento no reductibles a la mera deducción estadística.

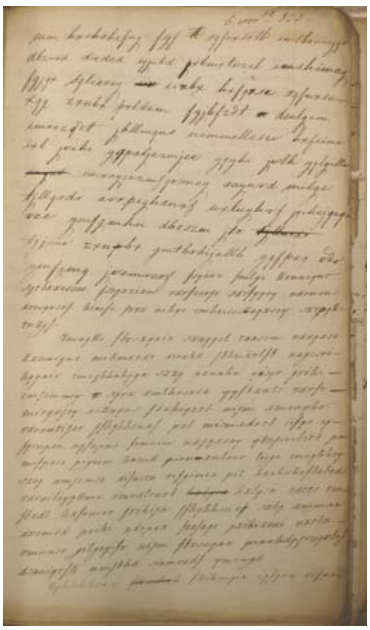

FIGURA 1. Primera plana de la carta de Michelena a la cancillería mexicana fechada el 6 de noviembre de 1824. AHDSREM, Legajo 1-1-44, f.81.

[9] Sobre la técnica y la historia de las frecuencias relativas, J. C. GALENDE DÍAZ, "Principios básicos de la criptología", *Documenta & Instrumenta*, 4 (2006), pp. 50-52; A. SINKOV, *Elementary Cryptanalysis. A Mathematical Approach*, Arizona, 1966, pp. 16-20; I. A. al-KADI, "Origins of Cryptology: The Arab Contributions", *Cryptologia*, XVI:2 (1992), pp. 97-127.

En casos como éste, la sustitución aplicada varía en función del sitio ocupado por cada carácter en el texto plano. Esa funcionalidad está determinada por la multiplicidad alfabética. El procedimiento efectivo de transformación se controla con una palabra clave (no es obligatorio valerse de una tal palabra en la generación de un criptotexto, mas lo normal es hacerlo cuando se trata de cifras polialfabéticas de la clase a la que pertenece el ejemplar considerado de Michelena). Todos los alfabetos a utilizar se colocan debajo del alfabeto de entrada, llamado también de definición, hasta generar en conjunto una especie de mapa. Cada elemento de la clave pertenece a uno de los, por así denominarlos, alfabetos inferiores, y la mecánica de su operación se resume así: localizar a cada carácter del texto plano en el alfabeto de definición y desplazarlo desde su lugar al de otro carácter en su propio alfabeto; de esta forma, la clave funciona cíclicamente para generar *n* cifrados de sustitución monoalfabética. Desde la estricta perspectiva de la técnica criptográfica, es indispensable que acontezca un desplazamiento de los lugares ocupados por cada carácter alfabético conocido para consumar efectivamente la sustitución.

Ahora, en un sentido elemental —aunque ciertamente autorizado por la comparación histórica de las diferentes reglas de transformación criptográfica— es adecuado describir a los criptosistemas polialfabéticos como un simple agregado de cifras monoalfabéticas de acuerdo con el venerable modelo de sustitución atribuido a Cayo Julio César, en donde cada letra de un texto plano se oculta con la letra ubicada tres, cuatro, o tantos lugares a su derecha como lo permita la longitud total del alfabeto único puesto en operación;[10] por ejemplo, usando el alfabeto español el desplazamiento no puede superar los 27 lugares; esto significa, en términos criptoanalíticos, que la clave necesariamente será algún número entre el 1 y el 27; pero esto indica que el llamado "espacio de la clave" es muy reducido, bastando 27 intentos para descubrir el número clave que, al restarlo del número representado por la letra cifrada, devuelve la letra del texto plano.[11] La vulnerabi-

[10] D. LUCIANO y G. PRICHETT, "Cryptology: From Caesar Ciphers to Public-key Cryptosystems", *The College Mathematics Journal*, 18/1 (1987), pp. 4-6.

[11] Su formación está basada en la aritmética modular. Es monoalfabética porque la clave, una vez elegida, configura un mapa al correlacionar cada letra alfabética con un carácter alfabético único. Por ejemplo, para encriptar la palabra "julio" con k=3 se convierte el texto plano a una secuencia de enteros, resultando 10 22 12 9 16; se agrega entonces 3 a cada integral, reduciendo el resultado modulo 27 si es necesario: 10+3=13; 22+3=25; 12+3=15, y así hasta obtener la cadena de integrales 13 25 15 12 19, que convertida en criptotexto es "MXNLR". Para definirlo formalmente, tenemos que $P = C = K = A27$, donde P es el texto plano, C la cifra, K la clave, y A el alfabeto único de definición. Para $0 \leq k \leq 27$, la definición del cifrado es ek(p)=(p+k)mod 26, y la del descifrado es dk(c)=(c-k)mod26, donde ($p, c \in A27$). A este tipo de aritmética se la llama agre-

lidad de un modelo de cifrado semejante, como se ve, es manifiesta. Y se trata, precisamente, del escollo supremo que se busca evadir con los polialfabetos.

Según lo anterior, parece de todo punto lícito ubicar al criptosistema utilizado por Michelena en la clase de los de sustitución polialfabética. Examinemos a continuación sus propiedades concretas.

Los pasos de encriptación se denotan por letras consecutivas a, b, …, z, y la clave dirige la selección de los alfabetos dispuestos en orden en una tabla. El uso repetido de la clave en tal sentido genera una encriptación polialfabética monográfica periódica. En términos llanos, vale decir que al repetir la clave en la forma expresada uno la hace "correr" sobre los grafemas del mensaje, lo cual determina múltiples combinaciones probables; ambos tienen una longitud de *n* letras, de manera que al combinarse para la sustitución producen un criptotexto de longitud *n*.[12] La letra de la clave que se empareja con la letra del texto plano indica el alfabeto de la tabla que se usará para cifrar esa misma letra. La evaluación histórica de estos detalles en el criptosistema de Michelena faculta para describirlo como una versión del modelo inventado por Giovanni Battista Belaso hacia 1553[13] —si bien debido a circunstancias los historiadores lo atribuyen a Blaise de Vigenère.[14]

Existe, sin embargo, una diferencia de aplicación importante entre la práctica que llevó a cabo Michelena y la que prescribía Belaso; para éste se trataba de escribir la palabra clave completa una y otra vez, transitando sin interrupción de una palabra a otra, por tanto, haciéndola cumplir en sí misma periodos completos; es precisamente la regla que Michelena no respetó. Para entender plenamente su manera de operar, solicito a mi lector observar la siguiente tabla:

---

gar modulo 27 o, simplemente, mod 27, donde el 27 se denomina la base. Para una breve exposición sobre el uso del modulo con las cuatro operaciones aritméticas básicas (aunque con algunas diferencias de nomenclatura) y su relación con la criptografía, véase J. B. READE, "Modular arithmetic and cryptography", *The Mathematical Gazette*, 72:461 (1988), pp. 198-202.

[12] D. LUCIANO y G. PRICHETT, "Cryptology: From Caesar Ciphers...", pp. 6-7; A. GRIFFING, "Solving the Running Key Cipher with the Viterbi Algorithm", *Cryptologia*, XXX (2006), p. 361. Sobre los polialfabetos, D. KAHN, "On the Origin of Polyalphabetic Substitution", *Isis*, 71:1, (1980), pp. 122-127, y *The Codebreakers*, New York, 1970, 135-136.

[13] F. L. BAUER, *Decrypted Secrets*, Berlin, 2002, p. 127. D. KAHN, *The Codebreakers*, New York, 1970, p. 137.

[14] D. KAHN, *The Codebreakers*, New York, 1970, pp. 145-148.

	a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*l*	*ll*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*
a	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z
b	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a
c	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b
d	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c
e	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d
f	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e
g	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f
h	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g
i	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h
j	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i
l	l	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j
ll	ll	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l
m	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll
n	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m
o	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n
p	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o
q	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p
r	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q
s	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r
t	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s
u	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t
v	v	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u
x	x	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v
y	y	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x
z	z	a	b	c	d	e	f	g	h	i	j	l	ll	m	n	o	p	q	r	s	t	u	v	x	y

Pertenece a una clase de matrices cuya principal justificación es facilitar y acelerar la sustitución polialfabética. Se ha discutido si es justo atribuir el diseño de *esta precisa* matriz, llamada en latín *tabula recta*, al ya mencionado Blaise de Vigenère, diplomático que contribuyó a la metodología particular del cifrado por sustitución. No obstante, generalmente se acepta hoy que la especie de *tabula recta* mostrada se forma, en general, de acuerdo con el criptosistema de Belaso.[15] Sea esto como fuere, parece lo más probable que Michelena debió apelar a un auxiliar muy similar o idéntico para cifrar sus despachos a mayor velocidad. Porque se antoja difícil imaginar a un diplomático, y en especial a uno situado en las circunstancias que le tocó vivir a él, deseoso de gastar tiempo cifrando sus despachos o notas letra por letra como resultado de sucesivas operaciones de aritmética modular o algún procedimiento matemático alternativo. Por supuesto, sólo podremos formular la mejor hipótesis tendiente a descubrir el modo real en que pro-

[15] Para una descripción del verdadero método de Vigenère, distinguido por imponer un pareo doble a causa de que las filas de la tabla forman pares, véase W. SCHUMAKER, *Renaissance Curiosa*, New York, 1982, pp. 123-124.

cedía cuando recuperemos y analicemos toda la documentación pertinente. Acaso en esa documentación irán insertas las reglas específicas de transformación criptográfica que muy seguramente le proporcionó la cancillería cuando lo envió a Londres. De hecho, una *tabula recta* como la que expuse arriba no cuenta entre los materiales compulsados por mí para desarrollar esta investigación, aunque mis pesquisas se han limitado a un puñado de archivos oficiales del gobierno mexicano en la ciudad de México. Dicha *tabula*, pues, la tuve que originar yo mismo en atención a las cualidades técnicas de los criptogramas analizados en este caso.

En definitiva, pues, actualmente juzgo como idealmente correcto el supuesto hipotético de que Michelena se valió de una *tabula recta* para cifrar con rapidez. Mas podría ser el caso que Michelena dejase a otra persona la dura tarea de cifrar sus textos; tiene sentido esta idea, pues a los diplomáticos de todos los tiempos normalmente los han servido amanuenses o secretarios; si esto es así, permanece la ideal corrección del supuesto citado, pues nada impide suponer que el amanuense o secretario tampoco tenía buenos motivos para desaprovechar una herramienta con la cual ejecutar sus obligaciones a la mayor brevedad posible.

Por otro lado, si dejamos de lado la esperanza en los hallazgos históricos eventuales para establecer hipótesis fecundas sobre este particular, basta con reparar en un solo hecho criptológico para estimar como teóricamente indudable que Michelena pudo servirse de una matriz de tipo belasiano para cifrar. El hecho, como quizá lo ha previsto ya mi lector, es que con dicha matriz *se pueden generar* criptogramas iguales al que ilustré con el fragmento citado de nuestro agente. Veamos esto con calma. Para fortuna nuestra, los documentos sí nos permiten saber cuál fue la palabra clave que utilizó Michelena: "Firmeza". Ensayé muchas veces con ella hasta descubrir que su función técnica era controlar sustituciones. Pero debí a la comparación del criptosistema en cuestión con ejemplares análogos la inferencia de que el tipo de sustitución era polialfabética. Y fue con el fin de asegurarme que tracé la *tabula recta* de 25 x 25 que se exhibe en una página previa. Apliqué, pues, la clave sobre el criptotexto y pronto noté que un pareo limitado a determinada longitud entre ella y cada carácter apuntaba infaliblemente, en el "mapa" configurado por la *tabula*, a la letra cifrada.

Eligiendo términos sencillos para facilitar la explicación, puede decirse que el alfabeto vertical en el extremo izquierdo de la *tabula* constituye el alfabeto de la clave, mientras el alfabeto horizontal en la cima es el alfabeto de definición o entrada, esto es, del texto plano. En el alfabeto de la cifra se elige la primera letra de la clave, en este caso F; a continuación, en el alfabeto de entrada se toma la primera letra de la palabra a cifrar, digamos H; entonces, partiendo de la F, se van

desplazando lugares hacia la derecha, y partiendo de la H lugares hacia abajo, siendo el punto de intersección de ambas líneas el carácter sustituto, M; hacemos lo mismo con la I, por un lado, y con la E, por el otro; encontramos, de manera por demás instructiva desde el punto de vista criptológico, que el sustituto vuelve a ser M. Esta circunstancia sólo se puede deber a la multiplicidad de alfabetos; y aunque el hecho, a primera vista, parece interpretable como una frecuencia capaz de delatar el empleo de un mero criptosistema monoalfabético, un análisis prolongado terminará por volver inútil semejante hipótesis; en efecto, una cosa es que se repita una letra en un mismo criptograma, otra cosa que con cada aparición *deba equivaler o representar* a un mismo elemento del texto plano. De este modo se puede apreciar el genuino potencial de los criptosistemas polialfabéticos para repeler el criptoanálisis —al menos uno centrado en el análisis de frecuencias—, en contraste con los monoalfabéticos.

Pero debo explicar cuál fue el uso *exacto* que Michelena hizo de su clave. La periodicidad en la repetición no es absoluta, pues al finalizar cada palabra del texto plano se suspende la inscripción de la clave, comenzando de nuevo en la siguiente palabra. Así, cuando nuestro diplomático se dispuso a cifrar el bigrama "He", sólo pareó con "He" las dos primeras letras de su clave, esto es, "Fi", y entonces localizó las sustituciones en los alfabetos correspondientes. A continuación, para encriptar la palabra "comunicamo" (es obvio que esto delata un error al cifrar, pero yo he decidido citar estrictamente por mis desciframientos)[16] no pareó con esa "c" inicial la "r" que ocupa el tercer sitio en su clave, sino la "F" inicial de "Firmeza", la cual continuó repitiendo completa hasta que "comunicamo" llegó a su final; entonces, nuevamente, repitió la clave desde el principio para controlar la localización de los equivalentes para cada letra del texto plano en los alfabetos de cifrado; podemos graficar este sistema con la siguiente rejilla binaria:

f	*i*	*f*	*i*	*r*	*m*	*e*	*z*	*a*	*f*	*i*	*r*
h	e	c	o	m	u	n	i	c	a	m	o

Al cabo, pues, la expresión "He comunicamo" terminó cifrada como "Mm hxehrhcfug". La rejilla nos asiste para concluir que Michelena aplicó su clave en una forma que recuerda el método inventado por Girolamo Cardano, donde la clave se genera a sí misma por los propios elementos del texto plano; más que de

[16] Véase nota 8.

una clave, pues, trátase de una autoclave.[17] Si Michelena hubiese deseado aplicar estrictamente el modelo de Cardano, habría utilizado "He comunicado" (tenemos que suponer la frase escrita sin errores) como la clave misma para cifrar "He comunicado". Pero es manifiesto que no lo hizo, y para probarlo el lector puede acudir a la matriz de 25 x 25 que configuré y buscar las coordenadas indicadas por el manejo de la clave en una forma, por así decir, intermitente; indefectiblemente conseguirá un resultado totalmente diverso al que arribó Michelena.

Los análisis antecedentes nos autorizan a concluir, así sea provisionalmente, que el criptosistema empleado por Michelena, en términos generales, estuvo constituido por una *tabula recta* de alfabetos estandarizados al estilo de Belaso —y aún, si se quiere, de Vigenère—, pero cuya clave funcionó más bien a la manera indicada por Cardano. Por lo demás, también podemos admitir como muy probable que él o un subordinado agilizó invariablemente la faena criptográfica con el apoyo de la *tabula*, escapando así desde un inicio a la mera perspectiva de tener que fatigarse con la práctica continua de algún algoritmo instaurado por la aritmética modular u otra rama de las matemáticas puras.[18]

Para terminar, es importante advertir un hecho innegable: Michelena se comunicaba con Lucas Alamán, el canciller mexicano; por tanto, Alamán tenía la obligación de conocer el mismo criptosistema de que se valía su subordinado. Ahora, el análisis intensivo de los pocos ejemplares cifrados firmados por Alamán que he podido acceder, incluyendo, por supuesto, la minuta del 12 de julio de 1824, me sugiere que nuestro Secretario de Estado también se facilitó la práctica criptográfica con el auxilio de la misma *tabula recta* de 25 x 25. Una diferencia crucial, sin embargo, reside en su personal manera de aplicar la clave. Alamán se pliega totalmente al modelo de repetición fijado por Belaso y la posterior versión modificada que se atribuye a Vigenère; esto significa que su clave se repite com-

[17] D. KAHN, *The Codebreakers…*, p. 144.

[18] Aceptando como parte de la notación n=25, donde n representa el cardinal (longitud) del alfabeto de definición, podemos operar con la fórmula de transformación lineal: $E_k (m_i) = m_i + k (_{i \bmod d})$ (mod n), que indica la presencia de una clave como medio de control en la función transformadora. La *d* representa a la clave; técnicamente representa la longitud de una secuencia de caracteres alfabéticos {k0, k1, …, kd-1}, es decir, todos los miembros de un conjunto finito *K* por el cual se configura la clave. Por último, m_i vale por el i-ésimo carácter o signo del texto plano. Ahora bien, operando con n=25 tal y como lo hizo Michelena, uno podría cifrar su despacho citado sustituyendo las incógnitas con los valores requeridos, conforme al siguiente ejemplo: E (H) = E (7) = (7+5) mod 25 = 12 = M. En efecto, si en el alfabeto de entrada la A ocupa el lugar 0, la H tiene que ocupar el 7 y la F, el 5.

pleta en todas las instancias de pareado, luego su longitud no varía en razón de la longitud de cada palabra del texto plano[19].

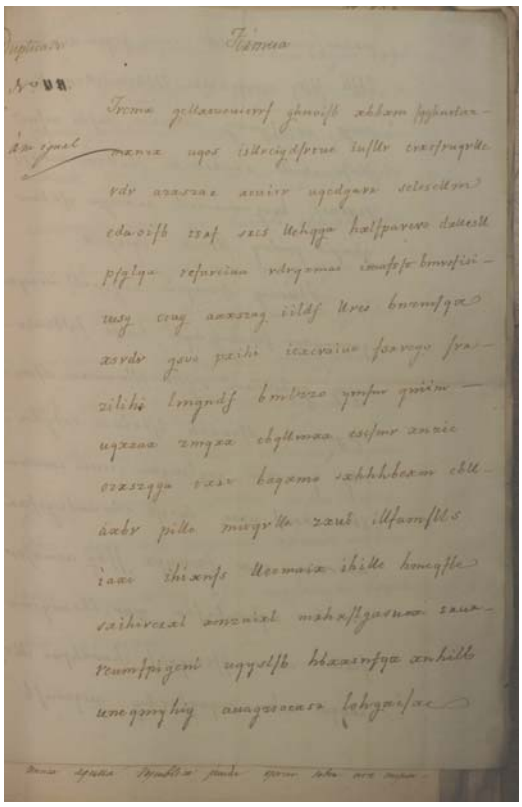

FIGURA 2. Fragmento de la misiva enviada por Lucas Alamán a José Mariano Michelena el 12 de julio de 1824. AHDSREM, legajo 1-1-44, f. 78.

Veamos un ejemplo de operación. El siguiente fragmento pertenece a la minuta recién citada del 12 de julio de 1824:

> En las negociaciones con Jano sobre reconocim
> iento de la independencia puede pretenderse
> que nuestra nacion de alguna garantta (*sic*)
> a la Jano para la posecion del Ahijado y otros
> payses de amereca (*sic*) que estan aun bajo su jobina
> cion (*sic*)

Transformado a cifra, su aspecto es el siguiente:

[19] W. SHUMAKER, *Renaissance Curiosa*..., pp. 124-126; D. KAHN, *The Codebreakers*..., p. 148.

Jvcmx gellxtueuitvvf ghnoifb xhbxm jqghntlaz
mxnzx uqos isllvcigdjvtue iujllv cvxtjvuqvlle
vdv azxszaz aeuitv uqedgavr selascllm
edaoifb tsrf srcs llehqga hxlfpavevo dxllesll
pfglqx vefuveiua vdvqxmas imafsjt bmvsfisi
yusg[20]

Ahora bien, el dato fundamental que virtualmente nos convence de que Alamán y Michelena usaron un mismo criptosistema, es que ambos aplicaron la misma clave, luego tuvieron que convenir en ella previamente. Sin embargo, es vital advertir, pues todo este análisis depende de ello, que Alamán no escribió "Firmeza" sino "Firmesa". Así se advierte en la figura 2. En mi opinión, sería ridículo explicar esto diciendo que el buen canciller tenía mala ortografía; Alamán era un hombre cultísimo, gran prosista según las reglas gramaticales y ortográficas de su época; es ridículo imaginar que pudiese equivocarse de una semejante manera sin notarlo. Así, creo lo más probable que su gesto de apuntar "Firmesa" representó una toma de licencia, digamos, para fortalecer al máximo el criptosistema contra todo eventual ataque de un espía; en una palabra, escribir y operar deliberadamente con "Firmesa" pone de manifiesto una inteligente previsión criptoanalítica.[21]

Podemos graficar la manera más elemental en la que Alamán pareaba los elementos a cifrar con los de su clave como sigue:

f	*i*	*r*	*m*	*e*	*s*	*a*	*f*	*i*	*r*	*m*	*e*	*s*	*a*	*f*	*i*	*r*	*m*	*e*	*s*	*a*	*f*	*i*	*r*	*m*
e	n	l	a	s	n	e	g	o	c	i	a	c	i	o	n	e	s	c	o	n	j	a	n	o

Guiándose con la *tabula*, pronto encontraría los caracteres para la cifra: Jvcmx gellxtueuitvvf ghnoifb. Para este caso, de nuevo, mi lector puede comprobar cómo varían las cosas si acude a la tabla y procura cifrar el mismo enunciado mediante el control de "Firmeza".

[20] AHDSREM, legajo 1-1-44, "1822-25. Reconocimiento de la Independencia de México por Inglaterra", ff.78-79bis. En los libros donde ha sido publicada se la presenta "corregida", etc.

[21] En efecto, si cualquier eventual interceptor de la minuta hubiese tenido la inspiración necesaria para adivinar la clave, seguramente lo haría en el sentido recto de su dicción; mas al esforzarse en aplicarla se toparía con obstáculos muy enojosos.

Una observación final. En el fragmento citado de la minuta de Alamán aparecen dos términos, "Jano" y "Ahijado", que sumergen en la perplejidad a quien, en virtud del desciframiento, puede leerlos por primera vez. Pero se trata, como fácilmente lo supone quien está familiarizado con la historia y la técnica criptológicas, de términos-código; "Jano" equivale a "España", "Ahijado" a "Cuba". Tenemos, pues, que en el particular espécimen considerado se ha sobrecifrado una codificación preliminar. Esta condición revela, sin duda, una complejidad interesante en el criptosistema puesto en marcha por tan sólo dos patriotas en los albores de la independencia política de México[22].

2. EL DIARIO RESERVADO DEL CORONEL JOSÉ ANASTASIO TORRENS EN COLOMBIA (1829)

A finales de noviembre de 1824 el coronel José Anastasio Torrens (1790-1857) fue sustituido por Pablo Obregón como Enviado Extraordinario y Ministro Plenipotenciario de México ante el gobierno de los Estados Unidos. Al nacer el año siguiente se embarcó en Filadelfia rumbo al puerto de La Guaira, en Colombia, para asumir funciones como secretario de la Legación Mexicana (Ignacio Basadre sería el oficial de la Legación).

Torrens siguió una línea de conducta muy poco tolerable para diversos personajes del ámbito gubernamental y diplomático colombiano. Era demasiado puntilloso en cuanto a formalidades protocolarias, interfería en asuntos oficiales internos del país que lo acogía, Simón Bolívar le merecía un afecto nulo y llegó a saberse, incluso, su disposición a colaborar con un grupo de intervencionistas extranjeros. En 1830, con la paciencia colmada, los colombianos hicieron lo necesario para que México lo reemplazara. El mismo Bolívar le devolvió sus pasaportes.

En toda esa época recurrió a la criptografía en múltiples ocasiones para transmitir noticias políticas o militares, opiniones y observaciones personales a sus superiores en la cancillería mexicana. Para ello se sirvió de dos expedientes técnicos, un criptosistema y un libro de códigos. En este escrito me ocuparé sola-

[22] Agregaré tan sólo que dichos códigos también forman parte de una lista más larga que complementa un criptosistema de diccionario localizado por mí en los archivos, el cual fue utilizado por diplomáticos mexicanos en la década de 1820. En un trabajo futuro lo daré a conocer.

mente de su operación con el criptosistema, esto es, un método de transformación a cifra estrictamente.[23]

En el Archivo de la Secretaría de Relaciones Exteriores de México constan las instrucciones originales para operar con el método en cuestión. En la siguiente transcripción he suplido por conjetura las fracciones ilegibles en el manuscrito, además de ajustar ligeramente la ortografía y la puntuación al uso actual con el fin de agilizar la lectura:

> La clave adjunta contiene siete renglones numerados al margen de la derecha y diez combinaciones en columnas numeradas arriba del primer renglón.
>
> Para cifrar con esta clave deben dividirse las palabras del texto en tantas fracciones cuantas permita el número de las vocales, de manera que a la vocal se junte la letra anterior o posterior y nunca la fracción se componga de más letras que dos. Estas fracciones se llamarán compuestas a diferencia de las simples, que sólo se compondrán de aquellas letras sueltas que en la palabra no puedan combinarse con vocal.
>
> Hechas estas fracciones compuestas y simples, se procederá a cifrarlas como se demostrará en el siguiente
>
> Ejemplo
>
> | Sa | n | ti | ag | o |
> |---|---|---|---|---|
> | 871 | 57 | 963 | 416 | 4 |
>
> La primera fracción *sa*, como que tiene *s*, la hallará en la 8ª combinación de la clave, y por lo mismo pondrá en la cifra el no. 8; y como que la *s* está en el séptimo renglón pondrá en seguida del 8 un 7; y viendo que la *a* pertenece al primer renglón, pondrá después del 8 y del 7 el no. 1, con lo que aparecerá un guarismo que dice 871.= Sigue la fracción simple *n*. Esta consonante está en la combinación 5, pues (sic) este número lo pongo debajo de la *n*, y porque esta letra está en el séptimo renglón pondré un 7 a continuación del 5, con lo que dirá 57

[23] He comentado brevemente un texto codificado de Torrens en mi artículo "Dos criptosistemas empleados por el coronel José Anastasio Torrens en Colombia (1825-1826). Una contribución a la historia de la criptología mexicana", de próxima aparición en el número 49 de las *Memorias de la Academia Mexicana de la Historia*.

esta partida.= Sigue la fracción *ti* cuya consonante, *t*, está en la novena combinación, por lo que pondré un 9, y porque esta letra se halla en el sexto renglón pondré a continuación un 6, y tocando la *i* al tercer renglón pondré un 3, con lo que dirá este guarismo 963.= Sigue la fracción *ag*, que está a la cuarta combinación, por lo que pondré un 4; y tocando la *a* al primer renglón pondré después el no. 1, y concluiré el guarismo con un 6, por ser el sexto renglón donde está la *g*, con lo que figurará este guarismo 416.= Finalmente, la *o*, con que concluye la palabra, se figura con un 4 que indica únicamente el renglón, pues que no está combinada una vocal con ninguna otra letra.

De esta manera quedará cifrada la palabra "Santiago" así:

871 57 963 416 4

Para descifrar viene el primer número de cada partida, y ése indica el número de la combinación, y el 2º y 3er número el renglón donde se hallan las letras de la combinación señalada por el primer número. Por ejemplo, en la cifra citada la primera partida es 871, pues (sic) el 8 me dice que en la columna octava está la combinación que busco, el 7 me dice que en el séptimo renglón, columna 8ª, está la *s*, y el uno me avisa que en el primer renglón está la otra letra, que será una *a*, luego 871 quiere decir *sa* cuya fracción pongo debajo de la partida, y observando el mismo método en todas las demás numeraciones quedará evacuada la operación de descifrar, sirviendo de gobierno que partida de tres números es de fracción doble, siendo de dos números es fracción sencilla de consonante, y siendo de un número solo es fracción sencilla de vocal.
[Rúbrica.][24]

En mi opinión, la descripción del procedimiento es lo bastante clara para no dar lugar a equívocos. La partición de los caracteres marca el paso esencial previo a la sustitución de los caracteres; tal sustitución puede ser monográfica o poligráfica. El fraccionamiento metódico que se prescribe no reproduce necesariamente la división silábica normal en el castellano (una propiedad que, probablemente, surgió al concebir el diseño como una guardia contra el análisis de frecuencias),

[24] AHDMSRE, exp. 5-16-8615, ff. 27-29.

de manera que los bigramas y trigramas del texto plano a cifrar, designados aquí con el término "fracciones", sólo de manera incidental terminan por confundirse con bisílabos o trisílabos regulares. Los conjuntos de dígitos que sustituyen a dichos bigramas o trigramas (pero también, claro, a los monogramas) reciben la denominación "partidas numéricas". No participa ninguna palabra clave para controlar la selección de los equivalentes en la cifra.

El componente fundamental del algoritmo es la siguiente matriz de 10 x 7 que la pieza transcrita lleva en apéndice (y al que su autor se refiere como "clave adjunta", manifestación de la típica costumbre de la época, por lo menos entre los usuarios diplomáticos de la criptografía, por considerar sinónimos a cifra, clave y aún código, tendencia cuya imitación sería hoy peligrosa desde el punto de vista técnico e historiográfico):

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
a	a	a	a	a	a	a	a	a	a	**1**
e	e	e	e	e	e	e	e	e	e	**2**
i	i	i	i	i	i	i	i	i	i	**3**
o	o	o	o	o	o	o	o	o	o	**4**
u	u	u	u	u	u	u	u	u	u	**5**
b	c	d	g	v	j	p	q	t	h	**6**
f	l	u	m	n	ñ	r	s	x	z	**7**

Al compararla con matrices análogas, en ésta destaca esa peculiaridad de reproducir las cinco vocales —ordenadas convencionalmente— del castellano en hasta cinco "renglones"; acaso el propósito del diseñador era nivelar las frecuencias relativas, de manera que al trazarse las coordenadas en la matriz para localizar el carácter en cifra —o, en sus términos, al "combinar" los dígitos para generar las "partidas" del ocultamiento—, un mismo grupo de dígitos no se repitiese tan a menudo. Sea esto como fuere, lo cierto es que Torrens pudo economizar en tiempo y esfuerzo al cifrar muchas comunicaciones reservadas y aún personales con este auxiliar a la vista, durante su estancia oficial en Colombia (o quizá el secretario de la legación, Basadre, lo hacía en última instancia).

Como ejemplo de operación presentaré un fragmento de su diario privado, fechado en Bogotá en octubre de 1829;[25] asiento en cursivas las partes ilegibles del texto que suplo conjeturalmente, y entre corchetes las partes descifradas; el lector podría ensayar con la matriz hasta conseguir las mismas versiones aclaradas:

> Sé positivamente que el Srio. de Relacs. Extes. ha escrito a mi gobierno para que me retire: según me habían informado ya y referí el 3 de agosto
> 27.473.87.474.865.2.827.26.773.563.4.271.264.475.573.261.263.547.
> 472.274.1061.363.26.1064.1064.3. [El mismo que escribió la comunicación me lo ha dicho hoy] y me confirma que es en virtud del informe de Gual que hizo en una comunicación que yo y otra persona (cuyo nombre no *tiene* presente) los habíamos dado muy malos contra el Presidente
> 827.962.537.363.563.365.4.1061.871.273.364.362.271.4.173.263.571.
> 3.764.77.2.874.57.4.765.2.362.361.77.472.264.763.1.762.774.472.106
> 1.363.26.1064.271.875.87.961.57.263.1. [este individuo ha salido de la oficina y por eso no puede darme copia pero me ha dicho la sustancia].
> 227.473.573.87.96.774.362.274.87.827.961.364.87.5.573.364.87. [El ministro de los Estados Unidos] me ha leído una carta que tiene preparada
> 3.362.162.361.773.663.77.1.164.273.561.77.265.517.364.262.872.527
> .227.2.662.77.263.263.4.362.875.87.175.57.263.4.572.87. [i debe darijirla (*sic*) a Bolívar cuando cese en el ejercicio de sus funciones] me lo ha comunicado en una *misi*va que me ha encargado guardar hasta que él crea conveniente publicarla. Entonces procuraré obtener una copia. Como
> 363.26.1064.473.453.87.96.774.227.265.517.964.1.271.87.473.771.87
> .362.164.273.561.77.3.1061.361.364.274.87.473.87.474.87.537.174.7
> 7.472.87.1.875.464.163.727.574. [dicho miuistro (*sic*)] es de la misma

[25] Diario reservado No. 18 de Torrens, en AHDSREM, LE-1700-II (7), "Colombia y México. Relaciones diplomáticas", ff. 404-406bis. Aunque ya se han publicado en libros varios mensajes aclarados que Torrens cifró con este método, es la primera vez —hasta donde sé— que se vuelve legible una parte de este "Diario reservado". En un estudio que publicaré próximamente los estudiosos podrán acceder al documento totalmente descifrado.

> opinión que yo el (*sic*) cuanto a las miras de Bolívar ha dado los mismos informes a su gobierno] trata de convencerlo de que ese plan no traherá (*sic*) ninguna ventajas a él ni a Colombia; por el contrario muchas desventajas: y diciéndole al mismo tiempo muchas cosas *duras*, sólo *supone* que un *favor*
>
> 865.2.26.772.865.2.574.827.227.873.574.875.87.1.462.57.962.87.865.2.174.77.471.57.2.874.87.76.271.572.87.873.57.875.264.57.872.57.963.473.527.964. [que cre que no es él sino sus agentes que forman esos planes sin su consentimiento].

Como se ve, Torrens separa con un punto cada "partida numérica", lo cual no recomiendan las instrucciones oficiales. Acaso adoptó esta estrategia deliberadamente, deseoso de evitar las repeticiones al cifrar bigramas o trigramas mientras sus ojos iban y venían de la matriz al papel sobre la mesa cuando era el turno de redactar en cifra ciertas partes de sus comunicados o su diario. Sin embargo, es técnicamente seguro que un acto similar puede abrir severas brechas en la seguridad del criptosistema.

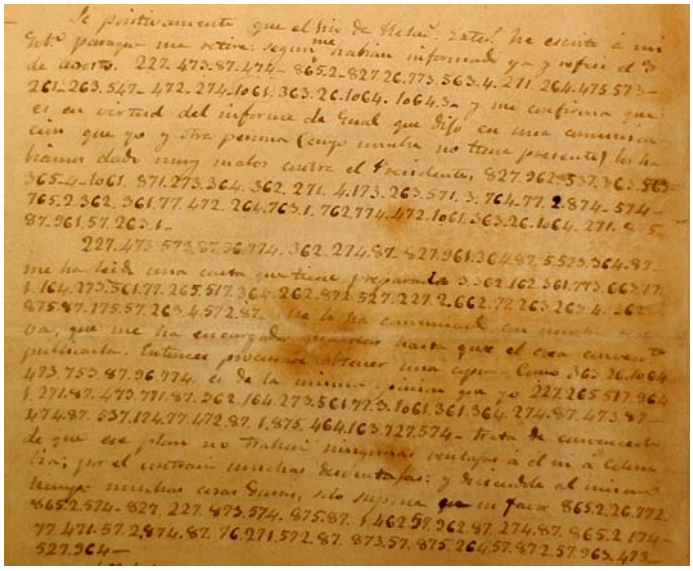

FIGURA 3. Detalle de la primera página del Diario reservado No. 18 de Torrens. AHDSREM, LE-1700-II (7), f. 404.

Para terminar, ofreceré algunos de los principales resultados que me devolvió un análisis comparativo de las propiedades generales de este algoritmo.

1. Exhibe rasgos característicos de la sustitución simple multipartita.[26] Para la comparación podemos limitarnos al célebre caso descrito por el historiador griego Polibio en el libro X (45-6 a 47-4 inclusive) de sus *Historias*.[27] Basado en un alfabeto griego quinario, el método se forma de una sustitución bipartita o bigramática. Modernizando y adaptando al español las condiciones para definir el alfabeto de definición, lo podemos representar gráficamente con una matriz de 5 x 5:

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Avanzando desde cada número en la columna de la izquierda o la fila en la cima especificado por cada una de las letras del vocablo a cifrar, situamos en la intersección cada equivalente críptico. De este modo, la palabra "lobo" se cifra "31 34 12 34". Es conspicuo el parecido formal y de funcionamiento técnico entre esta matriz y la de Torrens, mas la comparación pierde sentido en cuanto reconocemos que el sistema de Torrens admite sustituciones mayores a las bigramáticas.

2. En cierta medida incorpora la sustitución poligráfica. Esta cualidad está determinada por cuanto no se restringe a la mera descomposición del texto plano en caracteres simples, como sucede con el modelo de Polibio (estrictamente mo-

[26] Esto es, donde se expresa una relación entre el conjunto de los términos del vocabulario de un texto plano, *P*, y el conjunto de los términos en el criptotexto, *C*, según la definición específica m=2, $P^{(1)} \rightarrow C^2$. Recordar que, conforme a la lógica de conjuntos, se supone que P y C constituyen conjuntos finitos no vacíos para todos los casos prácticos.

[27] POLIBIO, *Historias. Libros V-XV*, Madrid, 1981, pp. 409-411. La propuesta de Polibio es "coger las letras del alfabeto ordenadamente y distribuirlas en cinco grupos de cinco letras cada uno", y utilizar cinco tablillas en donde se hubiera grabado las diversas secciones del alfabeto. Estaba planeado para funcionar en el campo de batalla cuando fuera urgente transmitir información "de manera muy exacta"; para operarlo se necesitaba que los grupos aliados en la liza indicaran por medio de antorchas las tablilla que se debía escoger y contaran con un telescopio de dos tubos para que el "receptor de la señal de fuego" pudiese mirar hacia los flancos izquierdo y derecho sin estorbos (pp. 409-410). Un esquema excelente de las tablillas en posición de cifrado se puede ver en el capítulo XX del clásico *Mercury, or The Secret and Swift Messenger* (Londres, 1641), de J. WILKINS, en la edición de L. LAUDAN, *The Mathematical and Philosophical Works of the Right Rev. John Wilkins (Two Volumes in One)*, London, 1970, vol. II, pp. 80-82.

nográfico). Ahora bien, recordemos que los criptosistemas, en general, se caracterizan por transformar cantidades fijas de texto plano en criptotexto —las cuales en la criptografía manual o clásica eran representadas normalmente por grafemas y, ocasionalmente, por grupos de dos o tres letras—[28]; es un hecho, sin embargo, que en la cifra de Torrens participa la sustitución por unidades simples y por bigramas y trigramas,[29] y como en ella se detecta la ruptura del texto plano en partes, resulta válido clasificarla *parcialmente* entre aquellas cifras donde el texto plano se organiza en bloques de igual tamaño mediando el control de una palabra clave. Así se procede con el famoso método Playfair que inventara Charles Wheatstone en 1854.[30] Pero hemos visto que en la cifra de nuestro coronel no participa clave alguna, por tanto, sus analogías con el Playfair apenas van más allá de reglamentar por lo menos un paso de encriptación basado en la partición bigramática.

3. Incluye rasgos característicos de los métodos tomográficos, también llamados de fraccionamiento y, más coloquialmente, "cifras bífidas". Un ejemplo puro es el que Félix Marie Delastelle publicó en 1902.[31] Bajo el control de una palabra clave, se opera una sustitución simple bipartita de uno a uno (esto es, monográfica) muy similar al caso de Polibio, pero complementada con una transposición de hasta cuatro lugares y la reversión de la misma sustitución simple bipartita. La encriptación total es autorecíproca, por lo cual se verifica una sustitución digráfica bipartita. Para descifrar se practica, en reversa, otra sustitución simple bipartita pero conjugada, de modo que el carácter autorecíproco desaparece. Las analogías entre este sistema y el de Torrens, pues, no son demasiadas, pero lo cierto es que ambas, en tanto generan cifras digráficas, se basan en transformaciones lineales, esto es, en matrices.[32]

---

[28] Los sistemas de trigramas o de conjuntos aún mayores gozaban de una reputación como altamente seguros, pero difícilmente se usaban porque hacían del cifrado una labor sumamente ardua.

[29] $P^{(n)} \rightarrow C^{(M)}$, con n>1.

[30] La tradicional es referirse a este método como "Playfair" debido a que su máximo propugnador fue Lyon Playfair, primer barón de Playfair de St. Andrews y gran amigo de Wheatstone. Se basa en bloques de dos letras y la encripación procede así: dada una palabra clave, inscríbase un alfabeto permutado de A_{25} (fue el alfabeto inglés que usó Wheatstone, aunque omitiendo la J del natural A_{26}) en una matriz de 5x5. F. L. BAUER, *Decrypted Secrets...*, p. 62. D. KAHN, *The Codebreakers…*, pp. 198-202. El sistema "Playfair" adquirió alguna fama en el mundo anglosajón a través de la literatura policial, en particular con la novela *Have His Carcase* de Dorothy L. Sayers, véase P. IBBOTSON, "Sayers and Ciphers", *Cryptologia*, XXV:2 (2001), pp. 81-87.

[31] En su obra *Traité Élementaire de Cryptographie*, véase D. KAHN, *The Codebreakers*, New York, 1970, pp. 242-244.

[32] F. L. BAUER, *Decrypted Secrets...*, 2002, p. 65. En un sistema poligráfico, un grupo *n* de letras de texto plano se reemplaza, como unidad, por un grupo *n* de letras de cifra. A. SINKOV, *Elementary Cryptanalysis...*, p. 113.

3. EL *NOMENCLATOR* DE LA LEGACIÓN MEXICANA EN ESTADOS UNIDOS DE AMÉRICA (1830)

En 1828 el puesto de Enviado Extraordinario y Ministro Plenipotenciario de México ante el gobierno estadounidense quedó vacante tras el suicidio de Pablo Obregón. Entonces el presidente Vicente Guerrero nombró como relevo a José María Tornel y Mendívil (1789-1853). Participante en la lucha por la independencia, orador, traductor y dramaturgo, Tornel y Mendívil fue diputado al Congreso de la Unión y ocupó varios puestos en la administración pública federal, por ejemplo, el de gobernador del Distrito Federal. Fungió como Ministro de Guerra y Marina en todos los periodos presidenciales de Antonio López de Santa Anna.[33]

Tornel recibió el pliego de instrucciones ordinarias y reservadas el 17 de noviembre de 1829. El presidente Guerrero le mandaba cifrar todas las comunicaciones reservadas y enumerar su correspondencia, exactamente como lo hicieran sus predecesores.[34] Tornel llegó a Washington el 5 de febrero de 1830 y cinco días después presentó sus credenciales. Eligió Baltimore como lugar de residencia, y si bien sus superiores, por motivos básicamente protocolarios, le pidieron que no se presentase como ministro, él ignoró la petición y vivió como tal. Entre sus encargos destacaba el de informar sobre las acciones del hijo del derrocado primer emperador mexicano, Agustín de Iturbide, y estar al tanto de los movimientos de Bolívar en Sudamérica. Después de algunos conflictos con personajes del gobierno y la diplomacia estadounidense, renunció a su cargo a principios de 1831.

Ciertos registros guardados en el AHDSREM indican como lo más probable que, para cumplir las instrucciones acerca del secreto en sus notas y despachos, se le entregó un *nomenclator*, esto es, un conjunto de caracteres que representan el vocabulario del criptotexto —logogramas o símbolos especiales que representan una palabra o frase, llamados variantes u homófonos (esto es, cualquier palabra del vocabulario del criptotexto asignada a una misma palabra del vocabulario del texto plano) para generar encriptaciones por sustitución monográfica o poligráfi-

[33] Tomo estos datos de la introducción editorial a J. M. TORNEL Y MENDÍVIL, *Breve reseña histórica de los acontecimientos más notables de la nación mexicana, desde el año de 1821 hasta nuestros días*, México, 1985 (edición facsimilar).

[34] Pero también se imponían esta disciplina los diplomáticos de otros países. El predecesor de Tornel, Pablo Obregón, era muy concienzudo tanto para fijar la cronología de sus despachos como para codificar aquellos que por su materia lo exigían. Para un estudio amplio del sistema codificador que siguió este ministro, véase mi artículo "Los despachos codificados de Pablo Obregón desde Washington (1825). Análisis y dos decodificaciones", de próxima aparición en la revista *Historia mexicana*.

ca— acompañada de una lista de términos código, es decir, frases que representan sílabas, palabras completas o nombres propios cuyo significado exacto se convenía entre los usuarios autorizados, de acuerdo con sus particulares necesidades de comunicación. (en ciertos ejemplares de *nomenclator*, al vocabulario del criptotexto y a los códigos se suma una serie de elementos llamados nulos, que nada significan pero se agregan a capricho con el propósito de confundir a cualquier tercero no autorizado en la comunicación).

En general, se puede afirmar que los *nomenclators*, o nomencladores, constituyen híbridos de cifra y código. En particular es adecuado definir al agregado de códigos en estos sistemas como un enorme alfabeto de cifrado donde la unidad básica de texto plano es la palabra o la frase.[35] Este método reinó virtualmente sin oposición en el Occidente desde desde el renacimiento hasta el amanecer de la época moderna,[36] por lo menos se observa históricamente que así fue en los Estados Unidos y muchos países europeos. Perdieron demanda cuando el siglo XVIII tocaba a su final y se desarrollaron alternativas de cifrado y codificación en conjunto que facilitaban la operación total de ocultamiento, en especial porque las listas de equivalentes, al formarse por una mezcla de homófonos y grupos numéricos, reducían considerablemente la extensión del sistema entero (en esa época los *nomenclators* podían alcanzar longitudes exageradas, lo que volvía difícil su manejo).[37]

Pero en México estas innovaciones eran desconocidas en 1830, si juzgamos por la clase de *nomenclator* que utilizó Tornel.[38] Se trata de un modelo con tintes

[35] J. C. GALENDE DÍAZ, "Principios básicos de la criptología"..., p. 53; BAUER, *Decrypted Secrets*..., pp. 18, 32-33; D. KAHN, *The Codebreakers*..., pp. XIV-XV. Este criptosistema recibió tal nombre por el oficial encargado de anunciar, en los palacios regios, los títulos de los dignatarios visitantes. La voz *nomenclator* (en ocasiones *nomenclador*) proviene del latín *nomenclātor*, *nomenclatōris*, compuesto con la raíz del arcaico *calare*, "llamar". J. COROMINAS, *Diccionario crítico etimológico de la lengua castellana*, Madrid, 1976, vol. III, p. 520.

[36] F. L. BAUER, *Decrypted Secrets*.., pp. 68-69. Un resumen de los mètodos esta clase que fueron usados en Inglaterra, Francia y España durante el XVI puede verse en J. W. THOMPSON y S. K. PADOVER, *Secret Diplomacy. A Record of Espionage and Double Dealing: 1500-1815*, Plymouth, 1937, pp. 258-260.

[37] En la práctica se inicia colocando las listas de códigos y sus respectivos equivalentes en dos columnas lado a lado; una lista es para codificar, la otra para decodificar. Todo esto pone de manifiesto una similitud formal y de sentido práctico entre los códigos de dos partes y los diccionarios bilingües. Se obtiene como ventaja principal que el decodificador puede acelerar su labor. Usuarios de estos fueron Thomas Jefferson, James Madison, James Monroe y otros "padres fundadores" en Estados Unidos, véase E. BURNETT, "Ciphers of the Revolutionary Period", *The American Historical Review*, 22/2 (1917), pp. 332-333; F. L. BAUER, *Decrypted Secrets*..., pp. 60-70.

[38] En México, sin embargo, y de acuerdo con la evidencia que he podido conseguir, se apelaba todavía a sistemas de sustitución monográfica muy similares o idénticos al *nomenclator* tradicional todavía en el primer tercio del siglo XX.

verdaderamente arcaicos. En la figura 4 se puede apreciar el sistema completo (el original forma parte de un despacho en el cual Tornel, siguiendo instrucciones oficiales, remite a la legación mexicana en Inglaterra una copia de su propia "clave" para normalizar el intercambio de información delicada con la legación en Baltimore).[39] Como se ve, la sustitución es exclusivamente homofónica[40]; se cuenta un homófono diferente para cada una de las 28 letra del alfabeto de definición elegido; 7 elementos de sustitución para 6 signos de puntuación (la coma, el punto, el punto y coma, los dos puntos, la interrogación y la admiración) y el paréntesis; 9 sustitutos para los números naturales del 0 al 9, y una lista de 59 términos codificados.

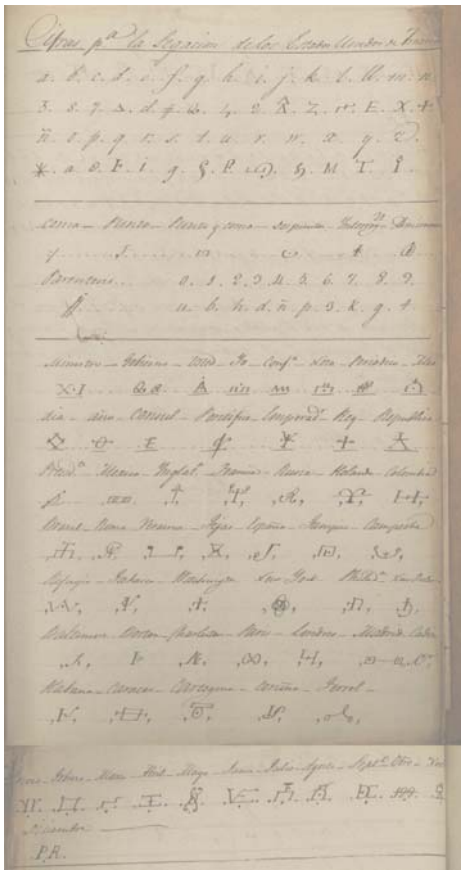

FIGURA 4. El *nomenclator* utilizado por José María Tornel en su correspondencia oficial desde Baltimore (1830). AHDSREM, Exp. 40-2-146, 2 ff.

[39] AHDSREM, Exp. 40-2-146 "Envían clave a la Legación de México en Londres, año 1830", 2 ff.

[40] No confundir con la sustitución polifónica se realiza por asignación de palabras del texto plano a una misma palabra del criptotexto. F. L. BAUER, *Decrypted Secrets...*, p. 35.

El tradicionalismo del ejemplar es tan patente, que se podrían señalar muchas analogías o, quizá, francas identidades entre los símbolos que participan en su formación y los de *nomenclators* históricos muy populares, en especial varios que circularon en ámbitos diplomáticos ingleses, franceses y españoles durante los siglos XVI y XVII. Por desgracia, no cuento con el espacio necesario para hacerlo. Tampoco me es posible exponer y analizar ejemplos de operación debido a que, hasta el momento, ninguno he localizado. Para llenar esta laguna será fructífero, quizá, poner en marcha tres líneas de investigación: 1) en los archivos estadounidenses donde se reúnan datos acerca de las actividades diplomáticas de funcionarios mexicanos en ese país (empezando, claro, con los National Archives); 2) en los legajos relativos a la legación de México en Gran Bretaña durante el mismo año de 1830 y después, por el fundamental motivo indicado ya sobre la clase de documento en donde hallé el *nomenclator* considerado, y 3) en los archivos de José María Montoya, individuo que sustituyó a Tornel como enviado extraordinario ante Washington, sabiendo que recibió la correspondencia oficial y las instrucciones reservadas de Tornel poco antes de asumir el cargo. Por motivos de comodidad y finanzas, actualmente me dedico a seguir las líneas de investigación 2 y 3. Confío en que no transcurrirá demasiado tiempo antes de transmitir, en el cuerpo de otro artículo, los beneficios descriptivos y analíticos de mis esfuerzos.